Securing Our eCITY

The Security Network®
Fostering Innovation Through Collaboration®

What "really" matters in Cyber?

(where common protections are needed for ALL
and your government product / service needs to accommodate them)

Can't happen to you?
6.5M Linked in passwords stolen…
Facebook hacks proliferate – contain hacker links, questionable "friends"
Yahoo email accounts hacked – almost 500,00 passwords compromised- etc, etc..

6 August 2012

Mike Davis

mike@sciap.org

EE/MSEE, CISSP, SysEngr
ISSA / TSN / SOeC… AFCEA / NDIA… IEEE / INCOSE / et al

ISSA Information Systems Security Association — San Diego Chapter

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
06 AUG 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
What 'really' matters in Cyber? (where common protections are needed for ALL and your government product / service needs to accommodate them)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **SCIAP,P.O. Box 131242 ,Carlsbad,CA,92013**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 2012 Navy Gold Coast Small Business Conference, 6-8 Aug, San Diego, CA. U.S. Government or Federal Rights License

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**34**	

What "really" matters in Cyber?

(B.LU.F.) (***and who says so?***)

- **OSD / federal S&T activities**
  - Distributed Trust
  - Resilient Architectures
  - Response and Cyber Maneuver
  - Visualization and Decision Support
  - Component Trust
  - Detection and Autonomic Response
  - Recovery and Reconstitution
- **NSA / agency S&T activities**
  - Mobility, wireless, & secure mobile services
  - Platform integrity / compliance assurance
  - End client security
  - Cyber indications and warning (I&W)
  - Mitigation engineering (affordability)
  - Massive data – (date centric security)
  - Advanced technology…. (targeted)
  - Virtualization – secure capabilities

It's NOT all about expensive new "cyber capabilities"

but more **about the SoS / I&I "glue"** (profiles, common EA, SoPs, standards, etc)

Along with **the basics**:
(1) enforced cyber hygiene,
(2) effective access control,
(3) reduced complexity in defense in depth IA / cyber,
(4) *continuous monitoring*
(which is NOT just audits!)

When in doubt, do the cyber basics well, then *develop critical / key needs* **(on slide 8)**

What are KEY cyber elements?

Fundamental issues…. (givens)

- Threats are illusive – so also plan around *consequences* (fault tree)
- *KISS, as complexity is our enemy – do the basics well (hygiene, anonymity, etc)*
- In a connected world, it's the *shared vulnerabilities* that will get you / us
- "They" have an *asymmetrical advantage*, so plan on it, leverage that
- *We must have a homogenous security protection in a heterogeneous world*

Essential gaps / needs…

- Follow the *OSD / NSA R&D / S&T perspectives*, they're authoritative sources
- Apply trade-offs / assessments from a *common end-state* (open world / ubiquity)
- Using an *enterprise risk management schema*, develop YOUR cyber action plan
- If you can't integrate "it" into your IT/network environment, "it" is useless
- Most of the gaps and needs are *"SoS" and "I&I" elements* (the "glue"), not "stuff"

If you don't know where you're headed, any path will do
Where the bad actors continue to count on us not being in sync

Threat Vectors of Interest

- **Mobile devices … and wireless** always predicted, *yet proliferates in 2012*
  - Start with more Android Trojans, digital wallets, USER provided network services!
  - Wireless security issues expand (besides 802.11 & WiMAX, to Zigbee, WirelessHART, Z-Wave, etc.) … ARM hacking increases
  - **BYOD** – many more hidden costs, legalities and risks than it seems on the surface…
- **Cyber crime: easy money, minimal downside and growing**
  - Illicit cyber revenues has essentially equaled all illegal drug trafficking $$$
- **Nation-sponsored hacking: When APT meets industrialization**
  - More targeted custom malware (Stuxnet -> Duqu is but one example and now *FLAME*!)
- **The insider threat is much more than you had imagined**
  - Coming from employees, partners, clients and compromised services and computing devices of all kinds. With Improved social engineering attack
  - social media critical data leaks / malware distribution
- **Misanthropes and anti-socials / hacktivism grows**
  - Privacy vs. security (and trust) in social networks. Radical group's DDOS attack can be effective on small businesses!

… mobile devices and cloud infrastructure hacking are likely the two of the biggest rising stars in cyber crime in 2012…

Threat Vectors of Interest (Cont.)

- **SSL/XML/web (HTML5)/browser vulnerabilities will proliferate**
  - Browsers remain a major threat vector (and bypasses the IA suite)
- **Hackers feeling the heat**… (the *easy* vulnerabilities are diminishing)
  - they need to invest in better attack techniques and detection evasion….
- **Cyber security becomes a business process…**
  - focused on data security, no longer a niche Industry…. EVERYONE will spin their capabilities
- **Convergence of data security and privacy regulation worldwide**..
  - Compliance even more so (PCI DSS, HIPAA, etc) .. *What is "good enough" security*?
  - Data security goes to the *cloud - where security due diligence is more than SLAs*!
  - IPv6 transition will provide threat opportunities… *Data Loss Prevention* is STILL key…
- **Containment** is the new prevention (folks now get the "**resilience**" aspect...)
- **Full time incident responders** needed, versus only virtual
  - Monitoring and analysis capability increase, but not enough (re: near real-time forensics &"chain of custody" evidence)…. "*continuous monitoring"* is KEY… (re: NIST docs)

There is MUCH to consider in the "threat" equation… and it's always changing
Hence why you must also practice "consequence" risk management

What are the major Threats?

*Which ones must we **all** "really" worry about?*

- **Summary of the top threats**
  - Malicious Code – viruses, botnets, etc
  - Stolen/Lost Laptop or Mobile Device
  - Spear Phishing – targeted SPAM
  - Unsecured Wireless Internet Networks
  - Insider/Disgruntled Employee

Where's your data?

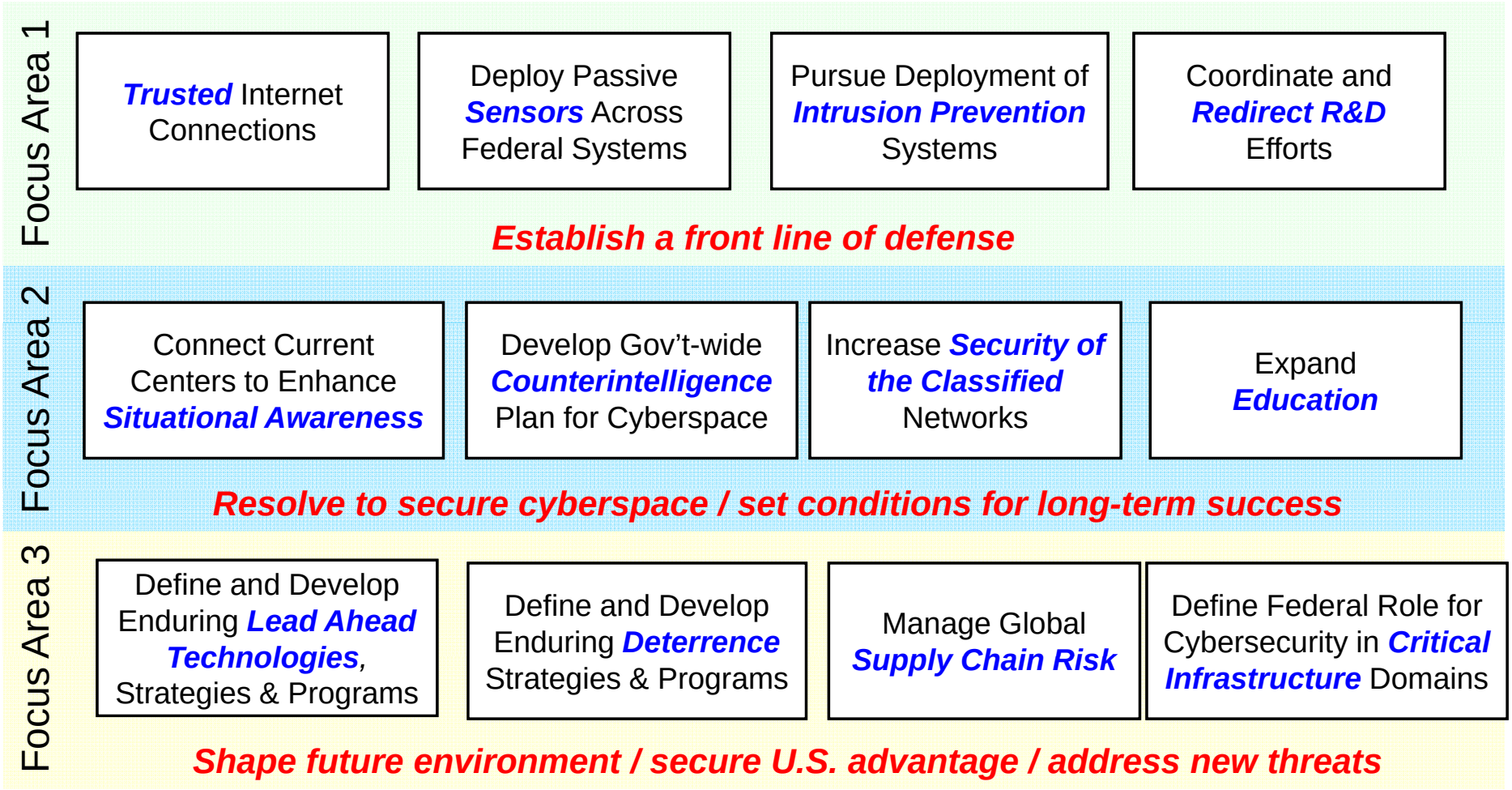
- **Key Business Security problems -** Computer Security Institute Survey (2008)
  - 42% reported laptop theft; 44% reported insider abuse; 50% detected computer viruses; 21% reported denial of service attacks; 20% reported systems being made bots

- **Survey of 10,413 information security professionals top threat concerns**
  - application vulnerabilities (cited by 73%),
  - mobile devices (66%) viruses and worms (65%) internal employees (63%)
  - hackers (55%) and contractors (45%) Other concerns include cyber terrorism (44%),
  - cloud-based services (43%), and organized crime (38%).

Basically Everything… So follow the risk consequences by practicing defense in depth – all affordably….

NSPD-54/HSPD-23: CNCI-1 '12 Initiatives'

(http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative)



Cyber efforts must synchronize with Federal Investments

The HARD part is implementing enterprise integration, interoperability *and controlling emergent behavior* - that can affect most focus areas

Prioritization of the Consolidated Enabling Technology Areas (*ETAs*)

high

- ***Distributed Trust***
- ***Resilient Architectures***
- ***Response and Cyber Maneuver***
- ***Visualization and Decision Support***

---

med

- **Component Trust**
- **Detection and Autonomic Response**
- **Recovery and Reconstitution**

---

low

- **Advanced Cross-Domain Solutions**
- **Advanced Cryptography**
- **Quantum Computing, Comms, and Crypto**
- **Biometrics**
- **Code Verification and Compliance**
- **Correct (Assured) by Construction Software**
- **Deception and Information Hiding**
- **Human Factors and Training**
- **Malware/Forensics Analysis and Reverse Engineering**
- **Resilient Infrastructure and Comms**
- **Scientific Theory and Measures**
- **Sensing and Data Fusion**
- **Software Pedigree and Provenance**

Source – QDR / DPPG study by OSD (Sep 2010)

CYBER is fundamentally about distributed trust & *secure messaging!*

Strategic Cyber Elements

(1) Collaborate on **common enterprise IA / cyber strategy and vision**
policy mapped to prioritized capabilities with assigned resources

(2) Develop common **overall enterprise risk assessment (ERA)**
accounts for both significant threat vectors & vulnerability consequences -> key mitigations
Organizational specific items complement and weighted within the existing CNCI-2 12 focus areas

(3) Align and **synchronize resources and cyber gaps / initiatives**
across federal organizations and tier 1 – tier 3 architecture perspectives

(4) **Address pervasive lack of basic cyber hygiene** enterprise wide
within the total claimancy's people, processes and products (technology)
enforce a scalable, global access control model, that preserves least privilege, "*attenuated delegation*"

(5) **Reduce complexity - Build a trusted cyber infrastructure**
on top of the existing IA/CND infrastructure, *as an integrated "SoS"* - with enforced CM
thus optimize our overall cyber package and ensure synchronization and *RESILIENCY*!

(6) **Better integrate / leverage education and 'proactive defense'**
"stealth offense" best left to law enforcement and qualified, undercover federal entities – covert / clandestine

Top down approach to a balanced, prioritized cyber execution plan

Key Tactical Thrusts

- Organize *national cyber security approach* / governance
- *Common ERA*, prioritize mitigations and resources
- *Begin Dynamic Cyber Enterprise Management* *(enforced hygiene)*

  *KEY capability – **effective continuous monitoring**!!!! (can't manage what you can't measure)*
- Top-down *enforcement of IA / Cyber* architecture
  - *Secure enterprise access control / Cyber IFF*
  - Overall Dynamic Cyber Defense (DCD) approach
    - Proactive / dynamic defensive I&W – monitor abnormal behavior
    - Virtual storefront – reacts quickly to predictive IO/IA I&W
    - IA/CND treated as an integrated "SoS" with lead/lag feedback
  - Common enterprise trust model (and implement TPMs, etc)
  - *Reduce complexity - IA Building blocks / APLs with pedigrees*
  - Integrate into an enterprise cyber security model / framework
- Effective lifecycle *awareness*, education, and training

95% security incident reduction

High ROI Activities that get us all moving quickly

Integration, execution is everything

as if you can't implement well, it costs you everywhere!!!

*The quantitative benefits of systems integration and interoperability (**I&I**) are*:

1. Shorter/reduced steps in business processes
2. Time taken to process one application/record
3. Less complaints from members of the public
4. No. of applications/records processed over a period
5. Less complaints from end- users
6. Reduced number of errors
7. Reduced software development time/effort
8. Reduced maintenance
9. Reduced no. of IT personnel

Until the user is happy using / benefitting from the new capability, it has no value

Buying stuff is "easy"
getting it to work in your environment is hard…

*The qualitative benefits of **I&I** are:*

1. Improved working procedures
2. Better communication with other related organizations
3. Job satisfaction
4. Redefine job specification
5. Improved data accessibility
6. One-stop service
7. More friendly public service

Plan for "I&I"
- Integration & Interoperability - then double it

The best capability means little, if it stays in the box

Cyber Security "Best Practices" Overview

(*Best practices are not a panacea, complete or only what you need to do – but a decent guide*)

- Quantify your business protection needs – do you have an asset inventory?
- Determine what is "good enough" or minimally acceptable for your business
- Quantify your environment's threats and vulnerabilities
  - your list should have 10 – 50 or so threats assessed – check out USCERT, others
- Have a **security policy** that's useful, complete, CEO/leadership endorsed
  - yes, that's *actually HAVE A POLICY*, profiles, access control, BYOD, etc then *enforce it*!
- Run self-assessments on security measures (use accepted tests, STIGs, PenTests, etc) and compliance (HIPAA, PCI, CFR, SOX, etc)
- Training and awareness programs – much needed, but not a guarantee
- **TEST** your continuity, recovery plans, **backup** – *have you ever you restored?*
- Encrypt where you can - asses where / how you need it : IM, e-mail, file transfer, storage, backup, etc)
- Be familiar with / USE the "NIST" IA/Security series – they are very good!
- **Reduce complexity** – use only approved / preferred products lists (A/PPLs)
- A **risk management plan (RMP)** - using both threats *AND consequences*

As, you can somewhat control what you plan,
but you usually ONLY get what you enforce!

What small businesses need to know about cyber security before they can offer services to the government

in general, *companies must provide a commensurate security level as the government site they are going to do business with*... (see NIST & GSA web sites below)

This **NIST** provides a good overview of the government requirements, which in general needs to be met by companies connecting to government sites iso services provided...
http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Information Security rules by **GSA**
http://www.gsa.gov/portal/content/104257

VA has a contract clause that's fairly standard
http://www.iprm.oit.va.gov/docs/Appendix_C.pdf

The **education department** has a good overview of requirements
http://www2.ed.gov/fund/contract/about/bsp.html

Government Contractors Now Subject to Cybersecurity Regulations –More are on the Way
http://www.scribd.com/doc/89226369/Government-Contractors-Now-Subject-to-Cybersecurity-Regulations-%E2%80%93-And-More-are-on-the-Way

Small business security overview (and detailed brief on the major security product details too)
http://www.sciap.org/blog1/wp-content/uploads/Small-Business-Security-ADT-Cluster-v4_Mike_Davis_July_26_2011.pdf

"Way Forward"

(given all the unknowns, variables… this is "one" *approximately correct* path…;-))

- **Vision** embedded…
  - know where you are going, where the passion is and what the USER values… as instantiated in your business success factors…
  - complement with SWOT / PEST opportunities.. Use centers of excellence, smart outsourcing, know your enemy / competition AND users well
- Risk Management Plan… **RMP**
  - A living document, current, dynamic, realistic, supporting your business metrics… as cyber *really* matters… *as you are betting your livelihood on it*
- Effective, working **Policy**…
  - Embedded in core business success factors, rules to enforce statutory, legal mandates, key processes, to enforce behavior (pos & neg incentives)
- **Basics**, *basics*, basics..
  - New toys matter little, if your environment is not maintained, monitored
  - *Poor hygiene / CM causes* MOST *security incidents* (*80%* (NSA) / 86-95% (Verizon))

SUMMARY
What "really" matters in Cyber?

- **OSD / federal S&T activities**
  - Distributed Trust
  - Resilient Architectures
  - Response and Cyber Maneuver
  - Visualization and Decision Support
  - Component Trust
  - Detection and Autonomic Response
  - Recovery and Reconstitution
- **NSA / agency S&T activities**
  - Mobility, wireless, & secure mobile services
  - Platform integrity / compliance assurance
  - End client security
  - Cyber indications and warning (I&W)
  - Mitigation engineering (affordability)
  - Massive data – (date centric security)
  - Advanced technology…. (targeted)
  - Virtualization – secure capabilities

It's NOT all about expensive new "cyber capabilities"

but more **about the SoS / I&I "glue"** (profiles, common EA, SoPs, standards, etc)

Along with **the basics**:
(1) enforced cyber hygiene,
(2) effective access control,
(3) reduced complexity in defense in depth IA / cyber,
(4) *continuous monitoring*
(which is NOT just audits!)

DO the cyber basics well, follow your RMP

Know your limitations / gaps , build in consequence risk management

IA/security resources

Main sites

This site has almost everything you need

https://infosec.navy.mil/docs/index.jsp

https://www.fleetforces.navy.mil/netwarcom/navycanda.

C&A moved to here

http://iase.disa.mil/ditscap/

other IA/Security sites:

https://www.us.army.mil/suite/portal/index.jsp

Great Sites too

http://csrc.nist.gov/

http://www.nsa.gov/ia/index.cfm

http://www.iatf.net/

other IA/Security sites (cont):

http://www.cert.org/

Great ISSE / SSE Site

http://www.sse-cmm.org/lib/lib.asp

http://www.commoncriteriaportal.org/

http://www.amc.army.mil/amc/ci/matrix/policy/policy_new.htm

https://www.sans.org/about/sans.php

http://iac.dtic.mil/iatac/

http://www.cerias.purdue.edu/

http://security.sdsc.edu/

http://iase.disa.mil/stigs/index.html

Begin with the end in mind

It's clearly important to understand the desired end result, instantiation of your vision - having the image of the vision as your frame of reference to evaluate everything else.
It is also impossible to integrate capability without having a plan and the correct systems in place to run the business.

Vision execution has to do with the "purposes" of capabilities, that have to do with visualization and complete planning! Bundled within personal and business: (a) leadership (what), (b) management (how), and (c) productivity (doing it well)…

You can take the concept further by **questioning the vision itself**!
Challenge assumptions, barriers, limitations, and obstacles…(the five whys?)

Always apply critical thinking (*reflective skepticism*) to the vision, as that brings New Ideas… Fosters Teamwork… Promotes Options… Uncovers Spinoffs… simulates a Clear Head… and fresh Perspectives emerge….

If you don't know where you are headed,
Seemingly blind alleys won't cut it either / waste $$$

Maximize investments / ROI

A strategic approach to maintenance and effectively using key performance indicators, organizations can better maximize resources, reduce capital and operating costs, and increase their return on investment (ROI). It's all about ***managing risk*****,** from a "high performance organization - **HPO**" operating perspective.

The critical elements of successful project value ROI analysis:

- Always starting with business goals and challenges versus technology.
- ROI analysis should be completed both for the past and the future.
- Business goals can not be achieved through technology alone.
- Project benefits cannot always be completely or accurately quantified, intangible elements have value too.
- There are many kinds of project costs in evaluations.
- Analyzing your entire technology project portfolio.
- Monitor critical business success metrics and re-evaluating your project alignment process.

Four ROI pillars: (1) strong foundation / operating plan, (2) defined enterprise effectiveness, (3) business enablement and (4) optimization / differentiation.

***Cyber ROI* is misleading - as it's more <u>insurance</u> than investment**

Drive out complexity - KISS

Complexity leads to *variation* in practice, opportunities for data / operational errors, and increased risk of *mission failure*.

Reducing complexity is key to improving both risk posture and productivity.

Human engineering and complexity theory teach that WE ALL need to *smartly, collaboratively:*
- Simplify - Standardize - Automate - Integrate

Reducing complexity is a major competitive factor for ensuring supply chain performance and exceeding customer expectations.
Given an increasing share of work is outsourced, the challenge of handling complexity has become all the more demanding.
Companies that do not master complexity risk experiencing supply chain inefficiencies, resulting in non-competitive working capital structures, lower transparency of cost drivers and difficulties in achieving service levels.
Address complexity in product, processes and organization.. and DATA

Use existing initiative to simplify both objectives and processes:
Just-In-Time… Standardization… Strategic Outsourcing…. Supply-chain management… Target costing… Performance Measures....

Take the "zero-baseline" approach to complexity

Cyber Security ROI

ROI is a big deal in business, but **it's a misnomer in security**.

Security ROI is difficult to compute, simply because it is hard to predict the probability of a true security event and the costs associated with the loss and mitigation of it.

A major issue in cyber security right now is that we've never been able to construct an intelligent return on investment (ROI) for cyber security.

As we've never been truly able to gauge how big the risk really is.

But, you need to be able to gauge the magnitude of the risk. what exactly the exposure is or if the actual event took place. because there just isn't enough good data.. There aren't good crime rates for cyberspace, and we have a lot less data about how individual security countermeasures—or specific configurations of countermeasures—mitigate those risks. We don't even have data on incident costs

The classic methodology is called annualized loss expectancy (ALE). Calculate the cost of a security incident in both tangibles like time and money, and intangibles like reputation and competitive advantage. Multiply that by the chance the incident will occur in a year. That tells you how much you should spend to mitigate the risk.

Cybersecurity ROI is considerably harder, as **the threat moves too quickly - so we can't create ALE models**. But there's another problem, and it's that **the math quickly falls apart when it comes to rare and expensive events**. … especially if the impact is huge, even low occurrence is very costly...

***Cyber ROI* is misleading - as it is insurance – a cost of doing business**

COTS / buy versus build

(Drive everything to a commodity state!)

MUST balance the business needs, shot-term and long-term goals, key requirements and available technologies and solutions on the market.

The company and key stakeholders must always consider and analyze all the options for each project and solution:

- Speed of implementation for a COTS vs. custom solution
- Cost of implementation of a COTS vs. custom build
- Functionality, flexibility and scalability in a COTS vs. custom build
- Support for COTS VS. custom build
- Organizational best practices, current technology and skill sets of employees
- Potential for upgrading, modification and replacement of COTS vs. build

Key elements in the process:

1. Properly analyze any COTS systems for suitability – the capability requirements and a technical perspective … *concurrent engineering* applies even more here
2. Beware the COTS sales pitch / trap to fall into is being promised functionality that isn't in the COTS at present but they will add for you.
3. Check for unit tests in the COTS and also what development practices they use, be wary if the vendor isn't giving much info about technical aspects. *Is the source code is available and have your programmers assessed it*?

Ultimately, If it's a critical business function do it yourself, no matter what

Key cyber capabilities to develop

(think "**secure comms / messaging**" - here proposed wrt *high tier examples*)

- **Distributed Trust --- Enable secure distributed interactions by establishing appropriate levels of trust among remote devices, systems, or users …. supports:** Models and Protocols for Trust Establishment; Infrastructure; Dynamic Evaluation; Out-of-Band and Physical Trust Maintenance

- **Resilient Architectures --- Enable functional capabilities to continue despite successful disruption or compromise by the adversary …. supports:** Morphing Engines Generating Unpredictability; Secured Network Storage; System Decomposition for Mission-Tailored Tools; Response and Cyber Maneuver

- **Visualization and Decision Support --- Enable human decision-makers to quickly understand the security and operational implications of the current situation and to rapidly ascertain the best course of action to pursue …. supports**: Real-Time Analysis Engines ; Common Operational Framework; Holistic Cognitive Environment

- **Response and Cyber Maneuver --- Enable defenders to perform shaping operations that minimize the attack space and frustrate adversary planning and to take action during attacks to block, disrupt, remove, or counter adversary actions. supports:** Polymorphic Technologies; Cyber Obfuscation; Network Agility

Net-centric Cyber Security = SoS and I&I aspects

CNCI

Comprehensive National Cybersecurity Initiative (CNCI). This initiative was launched by the second President Bush in National Security Presidential Directive 54 and Homeland Security Presidential Directive 23 back in January 2008.

there are 12 mutually-reinforcing initiatives that are intended to establish a front line of defense against today's immediate threats, to defend against the full spectrum of threats, and to strengthen the future cybersecurity environment.

INITIATIVE #1 -- Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections. This is about consolidating our external access points and creating common security solutions across agencies.

INITIATIVE #2 -- Deploy an intrusion detection system of sensors across the Federal enterprise. This is a passive system that watches traffic and helps notify us about unauthorized network intrusions. DHS is deploying signature-based sensors as part of the EINSTEIN-2 (PDF) capability, with notification going to US-CERT.

INITIATIVE #3 -- Pursue deployment of intrusion prevention systems across the Federal enterprise. This takes it up a notch with EINSTEIN-3 (PDF) and not only detects intrusions, but actively prevents intrusions into federal systems. This will have serious zero-day and real-time counter-threat capabilities.

INITIATIVE #4 -- Coordinate and redirect research and development (R&D) efforts. This initiative serves to help us get all of our R&D efforts working together, with a better communications and tasking infrastructure. It's an important part of utilizing our resources and our smartest people to the best of their abilities.

INITIATIVE #5 -- Connect current cyber ops centers to enhance situational awareness. This is our key threat-data sharing initiative.

The National Cybersecurity Center (NCSC) within Homeland Security is helping secure U.S. Government networks and systems under this initiative by coordinating and integrating information from the various centers to provide cross-domain situational awareness, analysis, and reporting on the status of our networks. As a side-effect, it's also designed to help our various agencies play better with each other.

INITIATIVE #6 -- Develop and implement a government-wide cyber counterintelligence (CI) plan. We're now coordinating activities across all Federal Agencies so we can detect, deter, and mitigate foreign-sponsored cyber intelligence threats to government and private-sector IT.

CNCI

INITIATIVE #7 -- Increase the security of our classified networks. Our classified networks contain our most valuable and most secret defense and warfighting information. We're continuing to work hard in securing these networks against the changing threat model.

INITIATIVE #8 -- Expand cyber education. This is where the Comprehensive National Cybersecurity Initiative begins to break down, because it's where all modern cyberdefense breaks down -- the people. We're training more and more cyberdefense experts, but we also need to expand that education up and down government, to corporations, and to individuals.
We can have the very best-trained cyberdefense expert in a corporation, say, and it'll all break down if the CEO won't allocate the time or funds to conduct that defense. It's all about making everyone know just how real these threats are.

INITIATIVE #9 -- Define and develop enduring "leap-ahead" technology, strategies, and programs. We'll talk more about future directions later, but the idea of leap-ahead is to get 5 to 10 years ahead of the bad guys and explore out-of-the-box thinking in building a better cyberdefense. This is good stuff, and it's the first CNCI initiative that, essentially, opens the door to concepts like Stuxnet (or what The Times claimed the White House called "Olympic Games").

INITIATIVE #10 -- Define and develop enduring deterrence strategies and programs. Put simply, because of the wildly asymmetric nature of the threat, we can't have a mutually-assured destruction option with cyberattack, the way we do with nuclear attack. We're working on developing deterrence strategies, but we're not there yet, a fact which is sadly all too evidenced by constant level of cyberattack, breach, and threat we find ourselves experiencing.

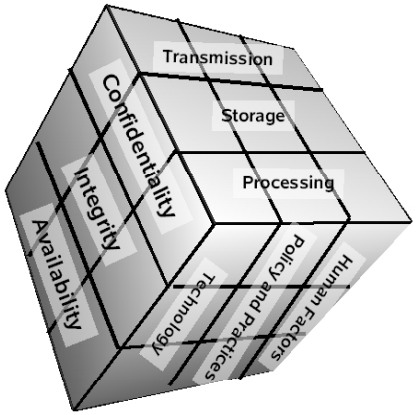
INITIATIVE #11 -- Develop a multi-pronged approach for global supply chain risk management. This area should be one of our biggest concerns. Most Americans get their computers from suppliers who use processors, motherboards, and components made outside the United States -- and often in China.
China, as we've seen repeatedly, is one of our most challenging "frenemies". They're clearly important to us financially, but they're also one of the leading sources of cyberattack (and, quite frankly, could be behind the one we're dealing with now). This initiative, though, isn't just about China. Our components and our supplies must be insulated from foreign influence and unapproved modification.

INITIATIVE #12 -- Define the Federal role for extending cybersecurity into critical infrastructure domains. The federal government is relying more and more on private sector services. For example, the Department of Interior is about to start using Google for its email infrastructure. This initiative encourages public/private-sector cooperation to extend Federal-systems cybersecurity into the wider cyber-infrastructure

What's a "simple" IA/Cyber vision / end-state look like?

AND what are the "requirements"?

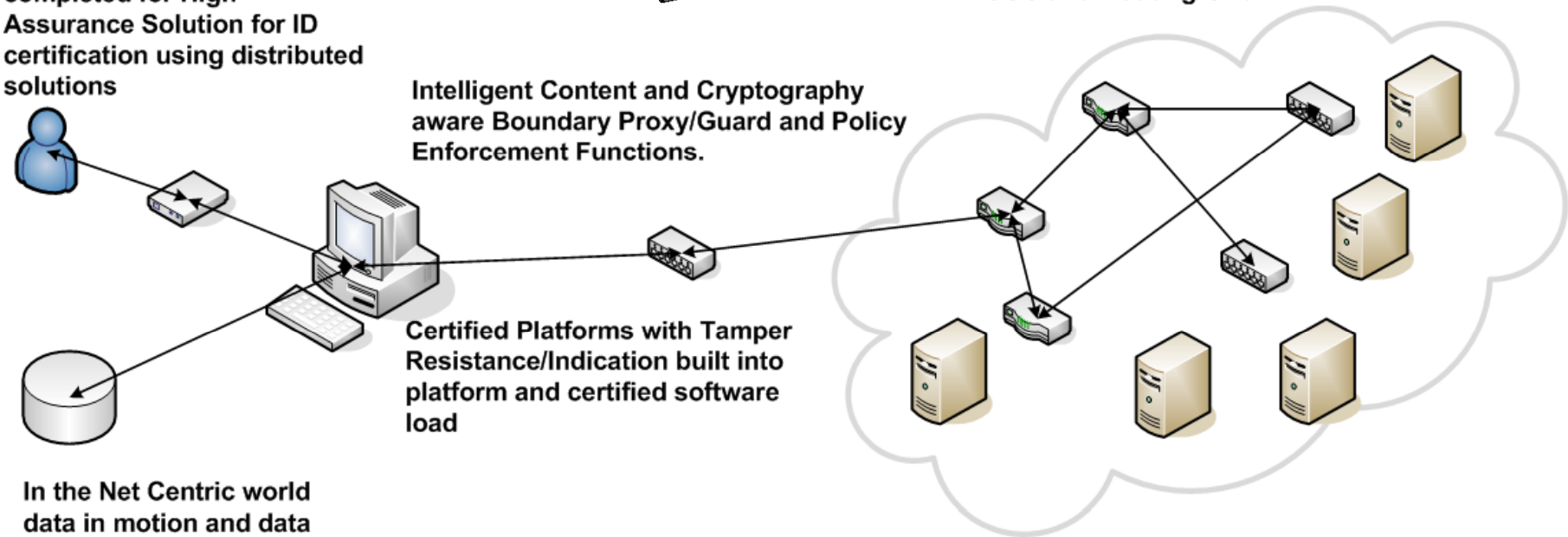
Notional Representation of IA Vulnerabilities and Architectural Approach to Layered Defense in a NetCentric World



Identity, access control and authorization are critical in this environment, significant work on distributed access control systems needs to be completed for High Assurance Solution for ID certification using distributed solutions

Protected Infrastructure, QOS, COS and Routing Grid

Intelligent Content and Cryptography aware Boundary Proxy/Guard and Policy Enforcement Functions.



Certified Platforms with Tamper Resistance/Indication built into platform and certified software load

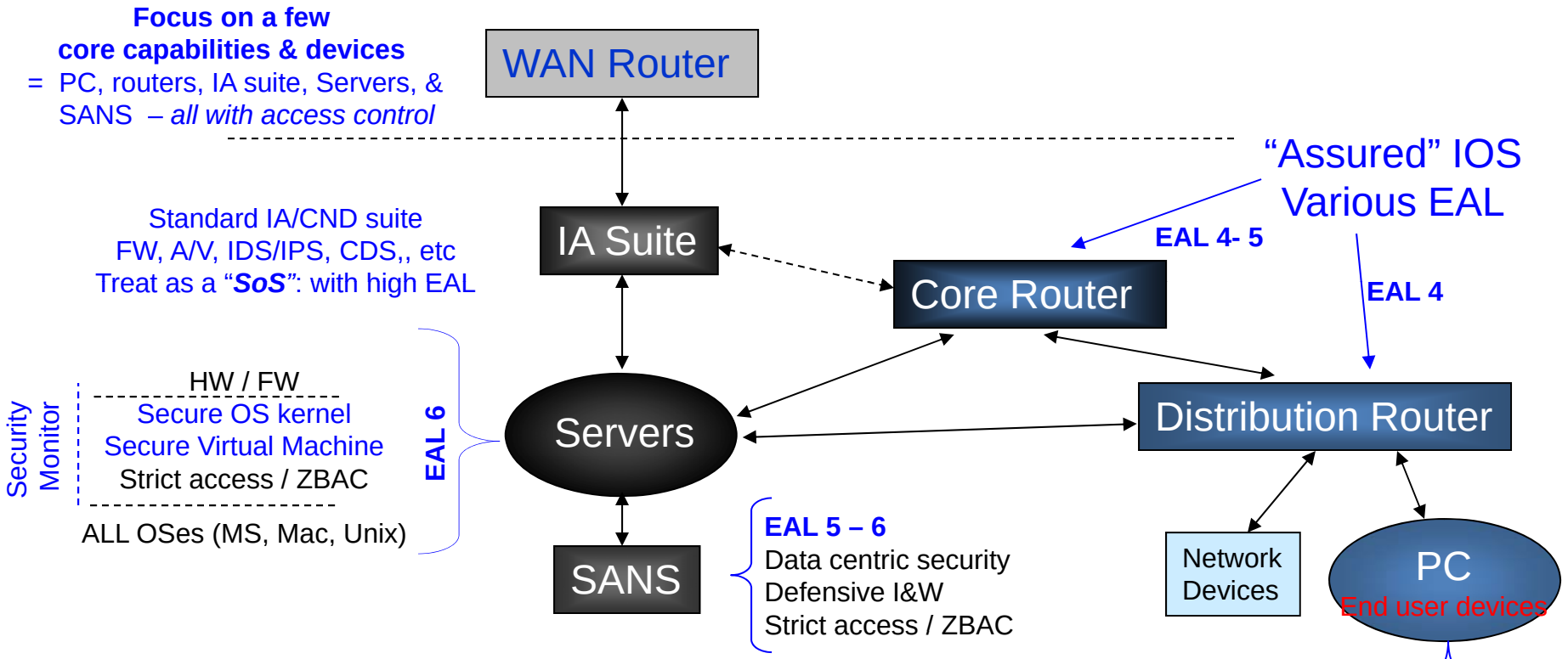
In the Net Centric world data in motion and data at rest become indistinguishable there is a need to protect storage, queues, and memory locations across the grid from information exfiltration.

Common Services from Geo Targeting to DNS must be protected at the level required by the highest risk applications using themyou cannot consume anything that you do not trust if affects your decision cycle in a way you cannot adapt to. Aggregate risk **compounds** the protection level required for the components and is **seldom** accounted for properly.

A cyber end-state stresses encapsulation through a secure virtualized fabric

Building a Trusted Cyber Infrastructure

"an *adequately* assured, affordable, net-centric environment"



Make IT security a commodity:

Use IA building blocks = APLs/PPLs -> "NIAP"

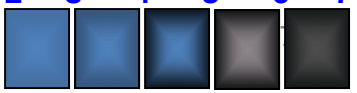
Interoperability and Compose-ability are built in upfront and help dramatically reduce complexity and ambiguity

Thus….establishing known risks & pedigrees:

Reduces attack surface, risks / impacts & TOC

Eval Assur Level (EAL):

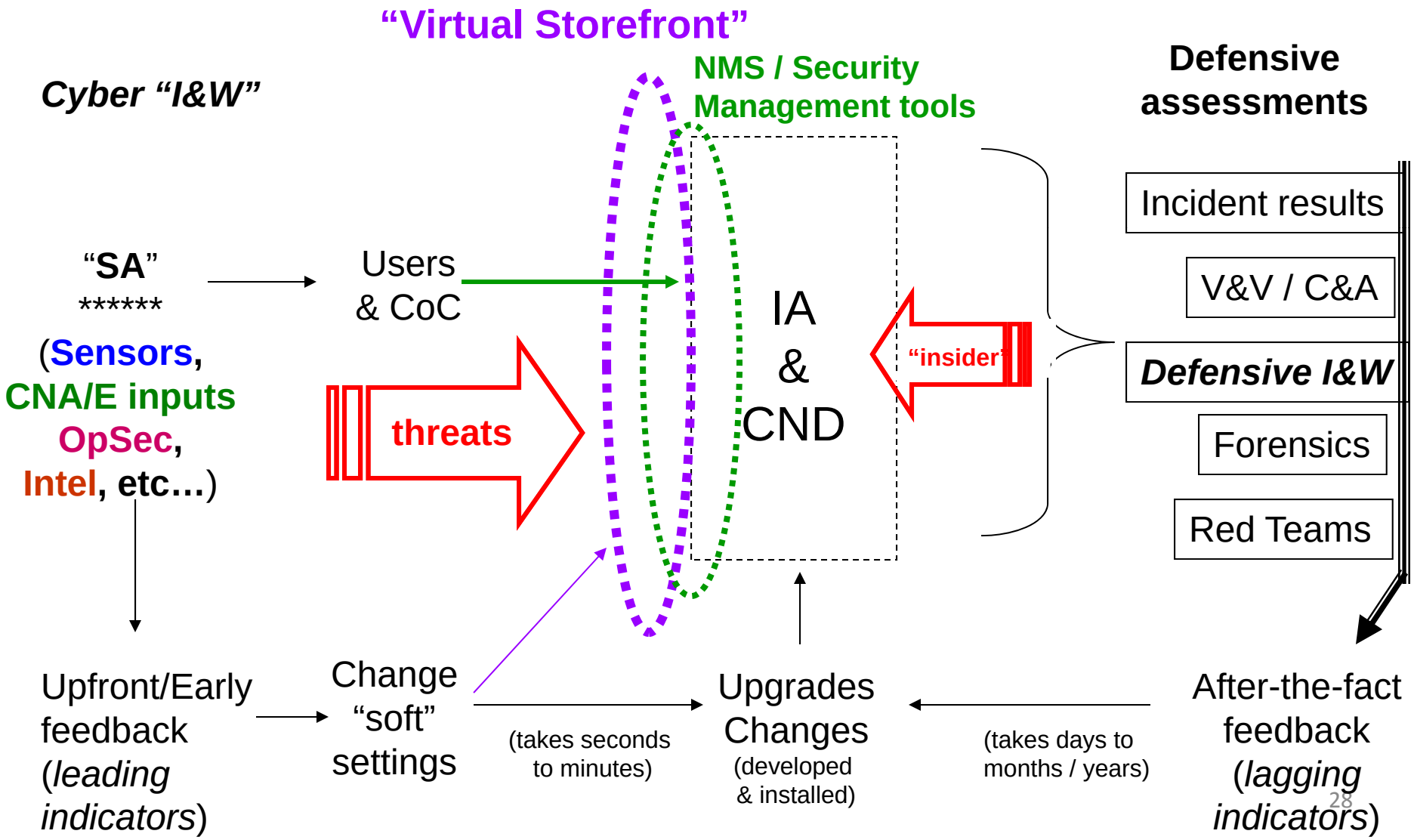
2 3 4 5 6 7



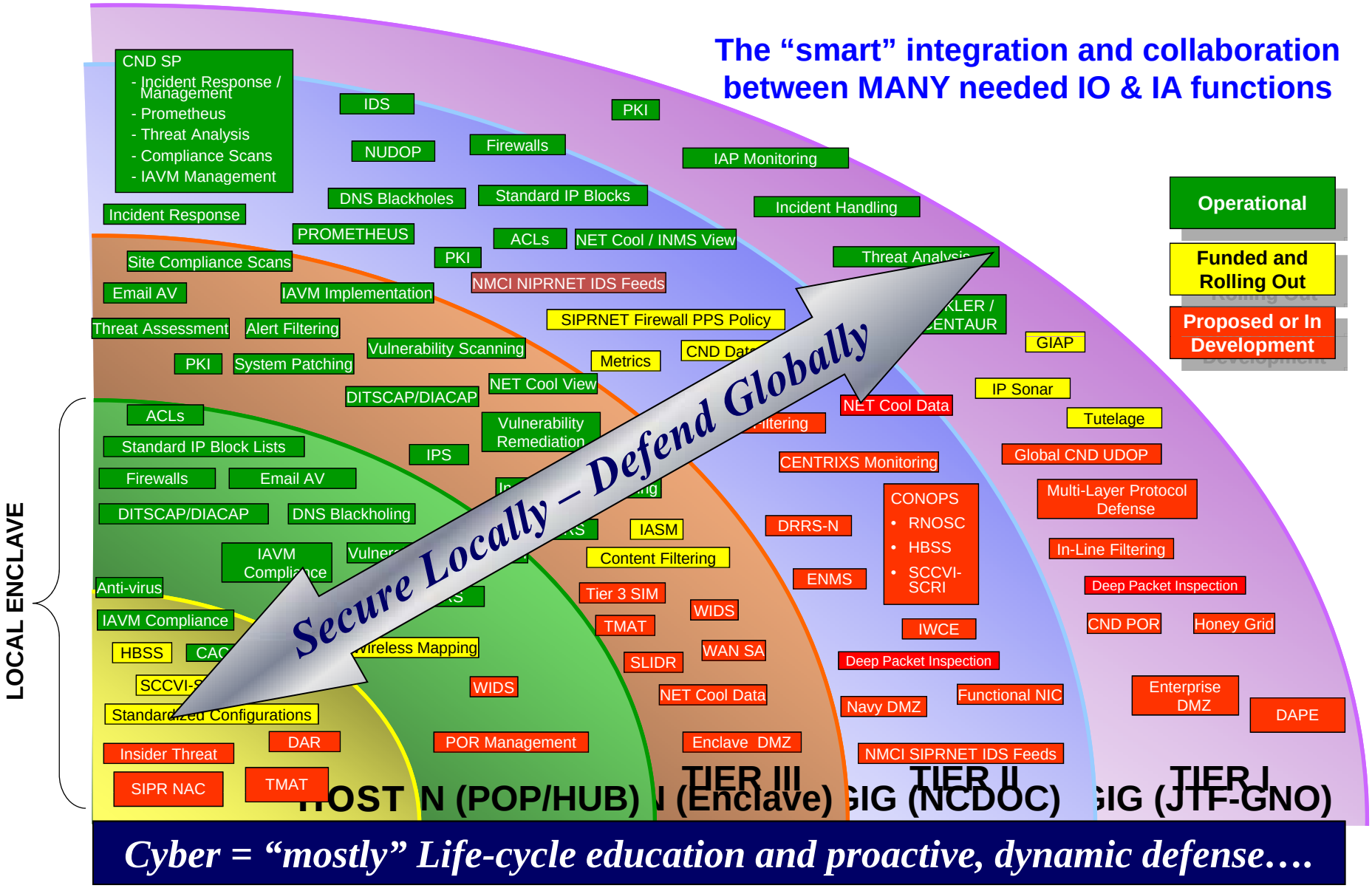
SO what are were trying to institute?

An integrated "Cyber" System using dynamic lead & lag feedback

Establish proactive, dynamic CND / IA Defense = ***dynamic cyber defense (DCD)***

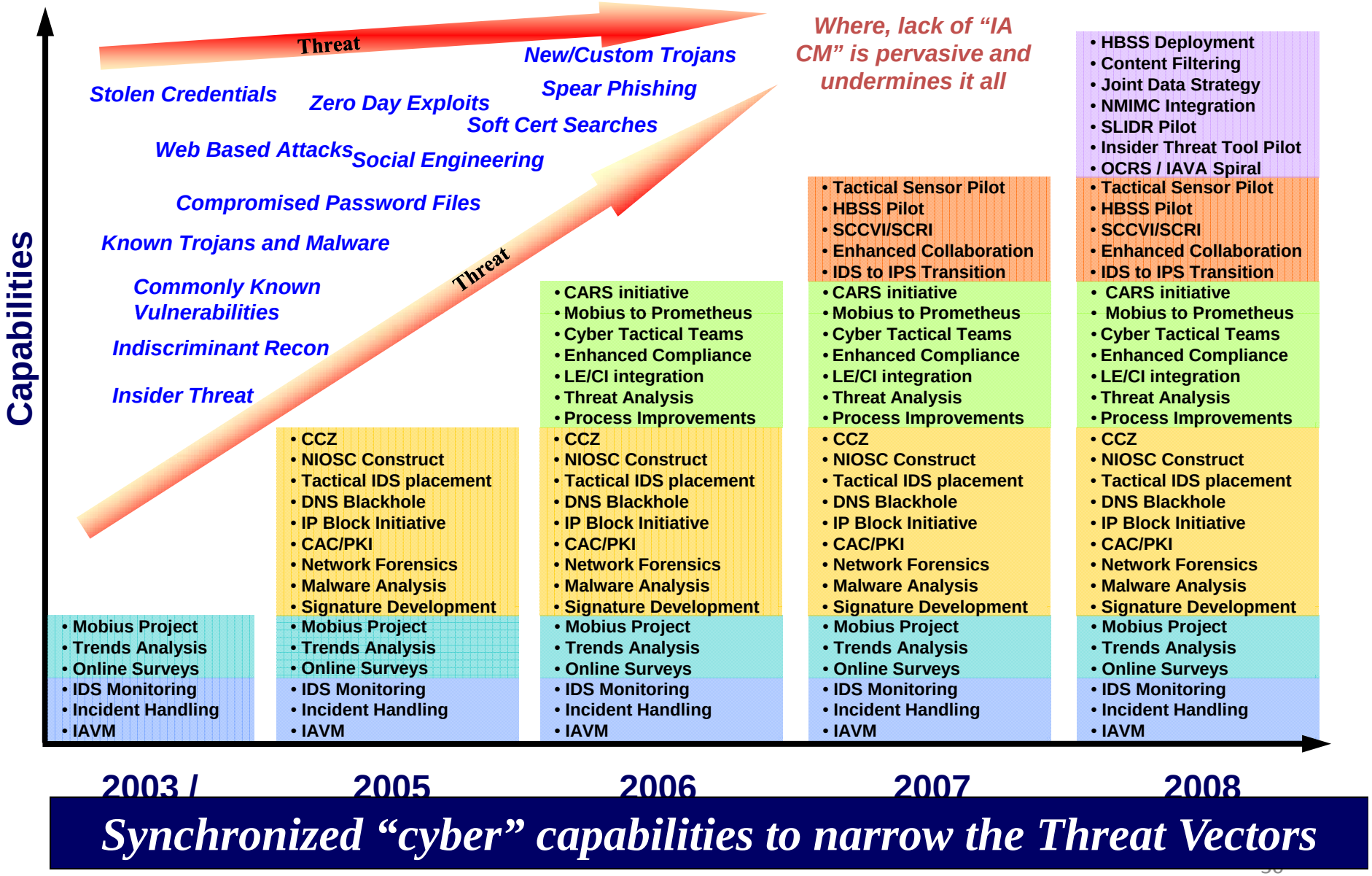


DoD CND (and "Cyber") Defense in Depth



(From NCDOC briefs)

Integration of Cyber Security and Defense

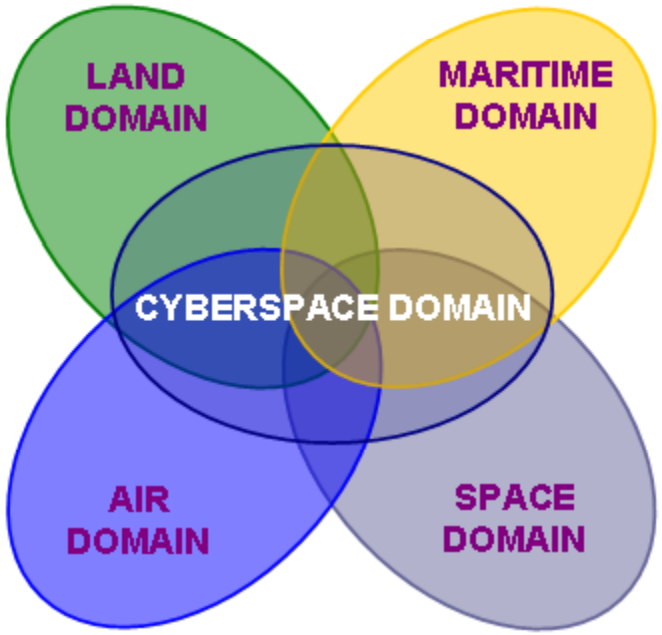


Synchronized "cyber" capabilities to narrow the Threat Vectors

(From NCDOC briefs)

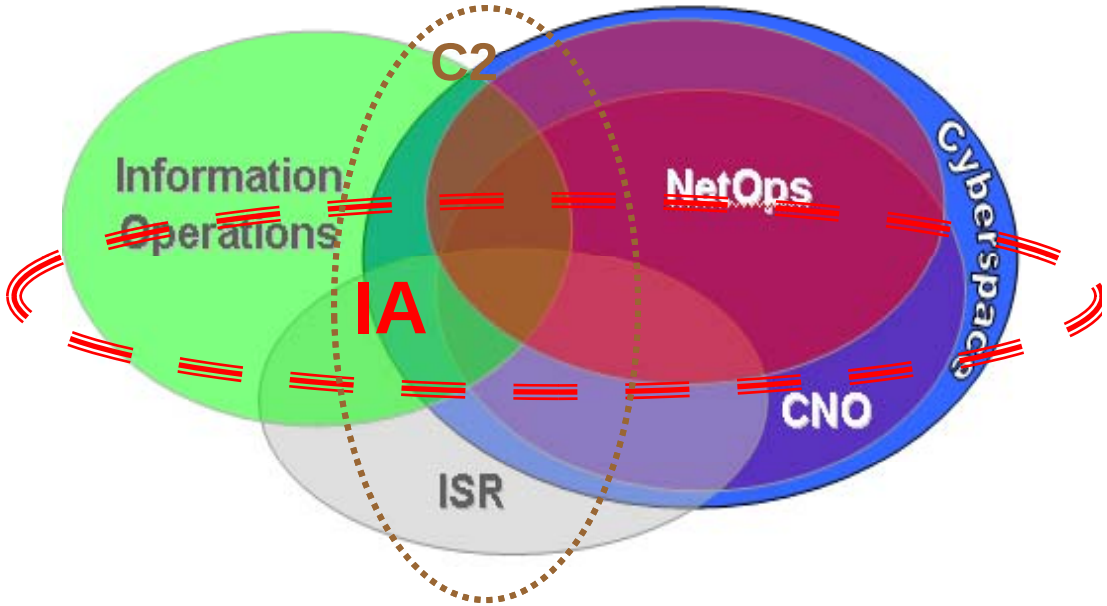
Cyberspace Characteristics

All of the warfighting domains intersect…



Cyberspace Domain is contained within and transcends the others

In relation to other mission areas…



… cyberspace is a blend of exclusive and inclusive ties

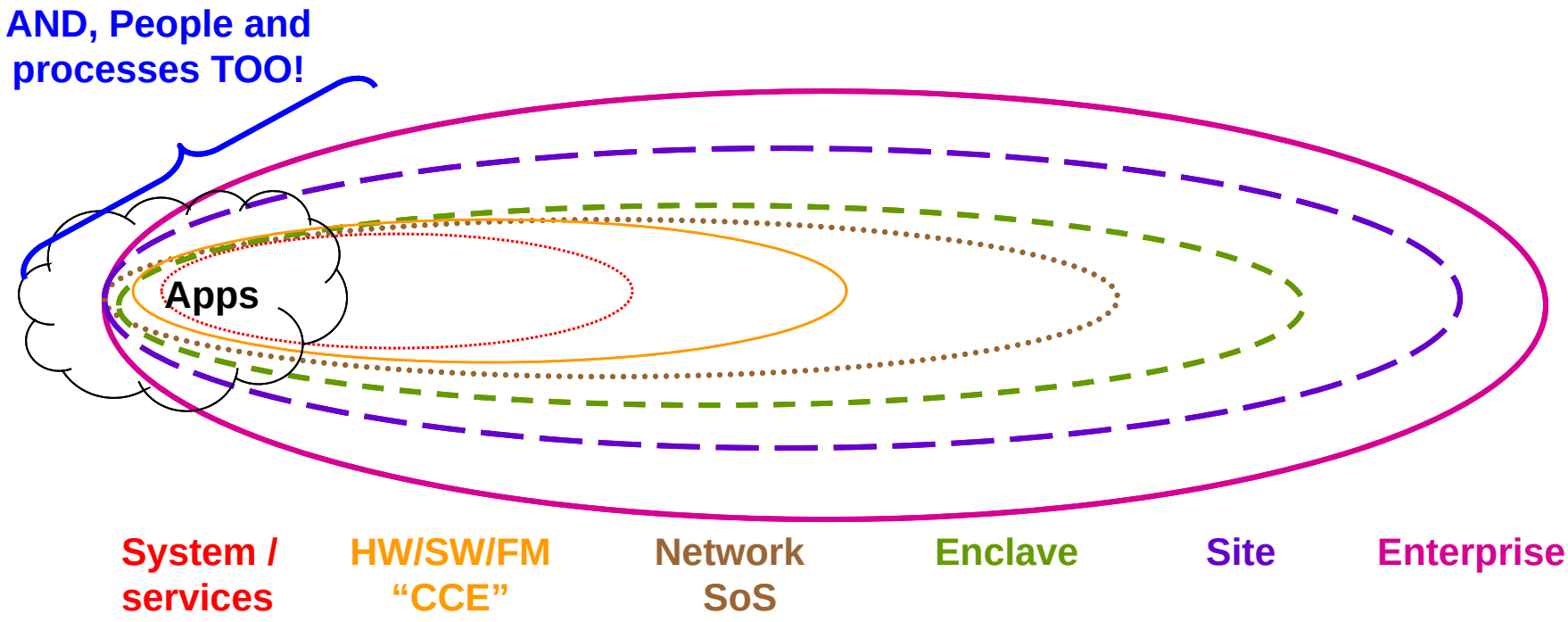
The "Venn connections / COIs" are extensive

Numerous dynamic "COIs" dominate relationships
Adding *complexity* and causing "*cross domain*" data sharing effects

(Source: derived from JS Cyber 101 brief)

IA / Cyber must be E2E!

WE have a "natural" hierarchy in our enterprise IT/network environment, where complexities arise in the numerous interfaces and many to many communications paths typically involved in end-to-end (E2E) transactions



Each sub-aggregation is responsible for the IA controls within their boundaries *and also* inherit the controls of their environment – need to formalize reciprocity therein!

Thus, the IA/cyber controls and interfaces in <u>each</u> element / boundary must be quantified / agreed to upfront!

So what really matters in IA/Cyber E2E?

A notional Quality of Protection (QoP) Hierarchy

(Wrt the *defense in "breadth"* position paper – **but what REALLY matters**?)

"**DATA** *QoP*"

(C-I-A and N & A)

Complex…
Dynamic…

IA&A **and** CBE / DCS

(distributed / transitive trust model … E2E **d**ata-**c**entric **s**ecurity and protections)

Settings

Core / **Security Services**

(WS* and other security **policy** / protocols / **standards** (including versions & extensions therein)

Standards

network protection – **CND** – FW / IDS / VPN / etc

(in general, mature capabilities – but multiple unclear "CM" processes are persistent and problematic)

IA devices

Known…
Static…

IO … **and** … IA

A&E / Policy

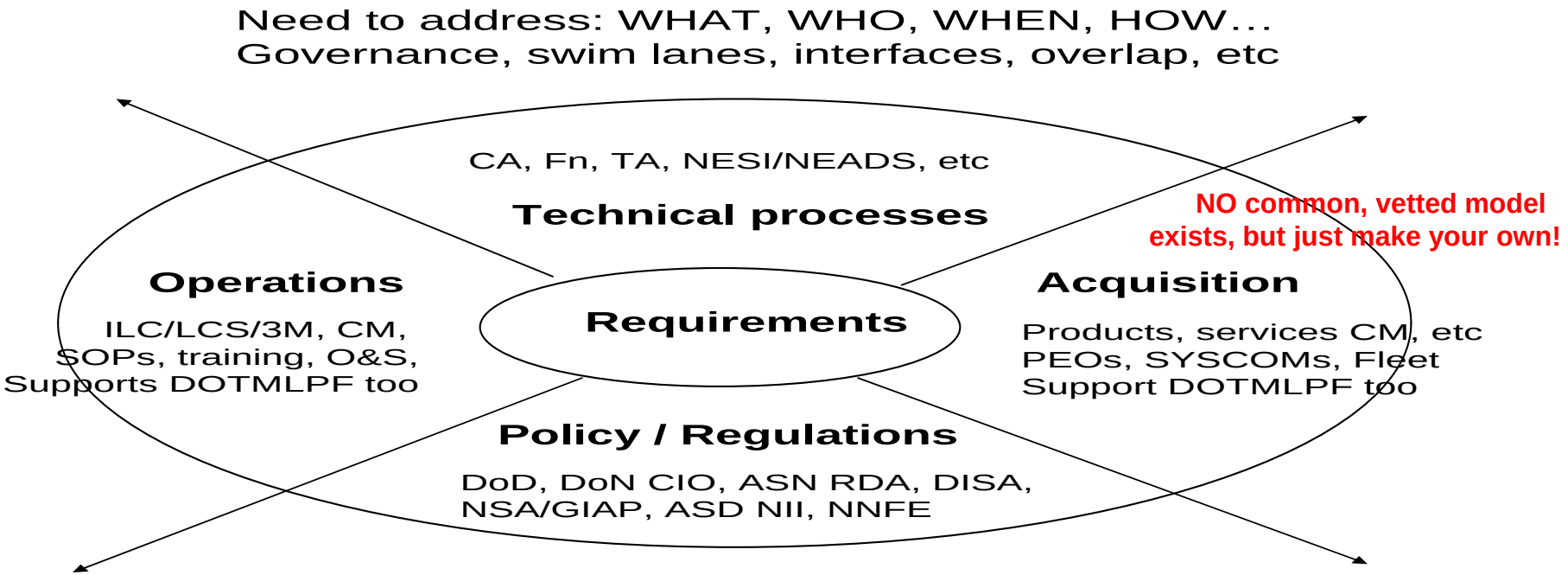
CNO/E/A, "I&W", OPSEC, etc

Crypto, KMI, TSM/HAP, policy, etc

Mainly: **IA standards, IA&A, CBE/DCS and digital policy!**

Is there a “cyber” equation / model?

(something for us all to “balance our risks / $$$)



Enterprise risk assessment (best value) = IA/SECURITY/CND (*defense*) (**a1**) + IO/CNE/CNA (*offense*)(**a2**) + SPECTRUM / TEMPEST (**a3**) + GOVERNANCE(**a4**) + REQUIREMENTS(**a5**) + THREAT / VULNERABILITIES (**a6**) + C&A / PEDIGREE (**a7**) + POLICY (**a8**) + TRAINING / EDUCATION (**a9**) + OTHER (**a10**) …. **AND** ???

“OUR” *risk management plan* should address *all variables*

The *sensitivity of the coefficients* will vary by company